UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/567,752 | 02/10/2006 | Paolo Abeni | 09952.0022 | 5634 |

22852 7590 01/15/2010

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

| EXAMINER | |
|---|---|
| SIMS, JING F | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/15/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/567,752 | ABENI, PAOLO | |
| | Examiner | Art Unit | |
| | JING SIMS | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *9/21/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) *1-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is responsive to communications: application 10/567,752 filed on 2/10/2006; amendment filed on 9/21/2009.

2. Claims 26-30, 32, 33, 36-45, 48-50 are amended.

3. Objection to the drawings has been withdrawn due to submission of drawings on 9/12/2009.

### *Response to Arguments*

4. In response to applicant's arguments that Lahtinen does not discloses "a response engine is triggered by an event generated by a pattern matching engine" on page 10 , lines 17-18, and Lahtinen does not discloses "a pattern matching engine ...[compares] the captured data with attack signatures for generating an event when a match between the captured data and at least one attack signature is found; and a response analysis engine [is] triggered by said event [to compare] with response signatures response data being transmitted on said network", Lahtinen in Monitoring of Data Flow for Enhancing Network Security discloses the aforementioned limitations in mostly in figures 2 and 6 and their corresponding description that can be found in paragraph [0028] to [0034], and [0057]-[0060].

5. Lahtinen discloses: a pattern matching engine *(i.e., fig. 2, block 230, finger print matcher block, and [0031], lines 18-20, fingerprint matcher block )*, comparing said the captured data with attack signatures *(i.e., [0031] lines 18, checks whether the HTTP data stream contains parts resembling known attack patterns, i.e. known*

*fingerprints)* for **generating an event** *(fig. 6, block 616, event classification)* when a match between the captured data and at least one attack signature is found *([0060], lines 1-3, if the result of the comparison is that the known misuse pattern are detected)*; and a **response analysis engine** *(fig. 6, block 616, analyzing and classifying the events)*, **triggered by said event** *(fig. 6, block 616, event classification)*.

### *Specification*

6. The Specification is objected to because it does not provide proper antecedent basis for the limitations "sniffer, implemented using the one or more computers", "a pattern matching engine, implemented using the one or more computers", and "a response analysis engine, implemented using the one or more computers" as recited in claim 1.

### *Claim Rejections - 35 USC § 101*

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. The 101 rejection to claims 26 is retained because of the reason listed below:

9. Although the preamble of the claim 26 recites "an intrusion detection system", the body of the claim does not positively recite any elements of hardware. The body of the claim recites that the "intrusion detection system" comprises three

components: “a sniffer”, “a pattern matching engine”, and “a response analysis engine”. In light of the specification, page 6, lines 25-27, “a sniffer” is a program, which directing “sniffer” to software per se. The type of media for "pattern matching engine” and “response analysis engine” are not disclosed in specification; however, to one skilled in the art, "pattern matching engine” and “response analysis engine” may be implement in software, therefore, directing to non-statutory subject matter. The recitation of “implemented using the one or more computers” in the claim does not overcome the 101 rejection for the reasons states above.

10. Claims 27-37 are rejected under 35 U.S.C. 101 because the claims depend on claim 26; however, they do not add any feature or subject matter that would solve any of the non-statutory deficiencies of the claim 26.

11. Claim 50 is rejected under U.S.C. 101 as being directed to non-statutory subject matter. Although the specification does not define the computer readable medium, it appears that the “computer readable medium encoded with a computer program product” may embody signals and carrier waves. As such, the claim does not fall within one of the four statutory classes.

### *Claim Rejections - 35 USC § 102*

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

**13. Claims 26-28, 30-32, 35-39, 41-44, and 47-50 are rejected under 35 U.S.C. 102(a) as being anticipated by Lahtinen (European Publication no. EP 1330095 A1).**

Lahtinen discloses:

**As per claim 26**, **an intrusion detection system** *(i.e., [0013], a flow monitoring mechanism enhancing system)*, implemented using one or more computers, for detecting unauthorised use of a network, comprising:

a **sniffer** *(i.e., [0014], lines 31-33, the system for the monitoring process; or fig. 2, block 220 host ID recognition block and/or block 222 client ID recognition, [0030], and [0031] lines 18)*, implemented using the one or more computers, for **capturing data** *(i.e., [0014], lines 31-33, identifying at least one response descriptor)* **being transmitted on said network** *(i.e., [0014], lines 32 and 34, data stream traveling from the server to the client, and traveling from the client to the sever)*;

**a pattern matching engine** *(i.e., fig. 2, block 230, finger print matcher block, and [0031], lines 18-20, fingerprint matcher block)*, implemented using the one or more computers, **for receiving data captured by said sniffer** *(i.e., [0031] lines 18, if the corresponding entry is not found, they forward the data stream to a fingerprint matcher block)* and **comparing said the captured data with attack signatures** *(i.e., [0031] lines 18, checks whether the HTTP data stream contains parts resembling known attack patterns, i.e. known fingerprints)* for **generating an event** *(fig. 6, block 616, event classification)* when a **match between the captured data**

**and at least one attack signature is found** *([0060], lines 1-3, if the result of the comparison is that the known misuse pattern are detected)*; and

a **response analysis engine** *(fig. 6, block 616, analyzing and classifying the events)*, implemented using the one or more computers and **triggered by said event** *(fig. 6, block 616, event classification)* for **comparing with response signatures** *(fig. 6, block 616 event classes; [0060], line 3-4, the event may be classified)* **response** *(fig. 6, step from 612 through 614 to 616)* **data being transmitted on said network** *([0059], [0060], the stream data)* as a response to said data matched with said at least one attack signature and **for correlating results** (fig. 6, block 616 event classification; and [0060], the even may be classified in the event classification step) of said comparisons with attack and response signatures for **generating an alarm** *(fig. 6, block 618 create alert; and [0060], lines 4-5, an alert is generated)*.

**As per claim 27**, the system of claim 26, wherein said response data is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network *(i.e. page 3, [0009], IP frame on TCP packets, target and destination port, for example)*.

**As per claim 28**, the system of claim 26, wherein said response data is captured by said sniffer by performing an analysis of both source and destination IP addresses in data packets transmitted on said network *(i.e. page 3, [0009], IP frame*

*on TCP packets, target and destination port, for example)*.

**As per claim 30**, the system of claim 26, wherein said response analysis engine generates the alarm when said response data indicates that a new network connection has been established *(i.e. [0044], the analysis of the response-request pairs)*.

**As per claim 31**, the system of claim 26, wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic *(i.e. fig 7, configured states, and [0032], a table of available state, and legitimate/valid request, for example)*.

**As per claim 32**, the system of claim 31, wherein said response analysis engine generates the alarm when a match between the response_data and a response signature identifying illicit traffic is found *(i.e. [0008], generates an alarm when something suspicious is detected in traffic)*.

**As per claim 35**, the system of claim 26, wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task *(i.e. [0068], configured states may include some known limitations for service which are known to cause false alarms)*.

**As per claim 36**, the system of claim 35, wherein said probing task verifies if any data has been detected on said network as the response to said data matched with said at least one attack signature and, if such condition is verified:

generates the alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine *(i.e. [0008], generates an alarm, and [0068], limits false alarms)*; or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine *(i.e. fig 1B, and [0009])*.

**As per claim 37**, the system of claim 36, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful *(i.e. fig 1B, and [0009])*.

**As per claim 38**, a method performed using one or more computers for detecting unauthorised use of a network, comprising:

**capturing data** *(i.e., [0014], lines 31-33, identifying at least one response descriptor)*, using the one or more computers, **being transmitted on said network** *(i.e., [0014], lines 32 and 34, data stream traveling from the server to the client, and traveling from the client to the sever)*;

**comparing the captured data with attack signatures** *(i.e., [0031] lines 18, checks whether the HTTP data stream contains parts resembling known attack patterns, i.e. known fingerprints)* **for generating an event** *(fig. 6, block 616, event classification)*, using the one or more computers, **when a match between the captured data and at least one attack signature is found** *(i.e., fig. 2, block 230, finger print matcher block, and [0031], lines 18-20, fingerprint matcher block )*; and

**when triggered by said event** *(fig. 6, block 616, event classification)*:

**comparing with response signatures** (*fig. 6, block 616 event classes; [0060], line 3-4, the event may be classified)* using the one or more computers, response **data being transmitted on said network** (*[0059], [0060], the stream data)* **as a response to said data matched with said at least one attack signature** (fig. 6, block 616 event classification; and [0060], the even may be classified in the event classification step); and

**correlating results of said comparisons (**fig. 6, block 616 event classification; and [0060], the even may be classified in the event classification step), using the one or more computers, with attack and response signatures for **generating an alarm** *(fig. 6, block 618 create alert; and [0060], lines 4-5, an alert is generated)*.

**Claims 39, 40, 42, 43, 44, 47, 48, and 49** are method claims corresponding to the system claims 27, 28, 30, 31, 32, 35, 36, and 37, therefore are rejected under

the same reasons set forth in the rejections for claims 27, 28, 30, 31, 32, 35, 36, and 37.

**As per claim 50**, a computer readable medium encoded with a computer program product loadable into a memory of at least one computer, the computer program product including software code portions for performing the method of any one of claims 38 to 49 *(i.e. NIDS runs on a server)*.

### *Claim Rejections - 35 USC § 103*

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**15. Claims 29, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen in view of Yadav (US patent publication no. 2003/0149888 A1).**

**As per claim 29**, Lahtinen discloses they system of claim 26;

However, Lahtinen does not explicitly discloses said response data is captured by said sniffer by analysing transport level information in data packets transmitted on said network;

Yadav discloses data packets have been transmitted on transport level *(i.e. page 3, [0034], an IDS may be implemented on network transport layer so incoming packets may be monitored)*.

Lahtinen and Yadav are analogous art because they are from the same field of endeavor of intrusion detection system by pattern matching.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and specify the packets are transmitted on transport layer as taught by Yadav because it would provide a standard way of packets exchanges at the time the invention was made.

**Claim 41** is method claims corresponding to the system claims 29, therefore are rejected under the same reasons set forth in the rejections for claims 29.

**16. Claims 33, 34, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen in view of Maher, III et al (US patent publication no. 2002/0105910) (hereinafter Marher).**

**As per claim 33**, Lahtinen discloses the system of claim 31;

However, Lahtinen does not disclose said response analysis engine comprises a counter which is incremented when a match between the response data and a response signature identifying legitimate traffic is found;

Maher discloses the limitation *(i.e. [0045], [0047], increment or decrement counter)*.

Lahtinen and Maher are analogous art because they are from the same field of endeavor of intrusion detection system by pattern matching.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and add an arithmetic logic unit to increment or decrement counter as taught by Maher because it would provide possibility of fine control over an objective subject.

**As per claim 34**, Lahtinen disclose when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm *(i.e. [0068], configured states may include some known limitations for service which are known to cause false alarms)*.

**Claim 45 and 46** are method claims corresponding to the system claims 33, and 34, therefore are rejected under the same reasons set forth in the rejections for claims 33 and 34.

***Examiner Notes***

Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part

of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/

Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437